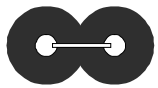
X.509 Policy Processing

May 13, 1999

Santosh Chokhani (CygnaCom)
Serge Mister (Entrust)
Tim Moses (Entrust)

Briefing Outline

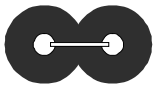
- **Motivation for change**
- **Business requirements**
- **Inputs**
- **Outputs**
- **Algorithm Overview**



CYGNACOM SOLUTIONS

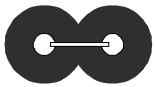
Policy Processing Change Motivations

- **Fix the policy mapping flaw**
- **Policy processing behavior should not depend on the criticality of the certificatePolicies extension**
- **Mapped policies should not be accumulated, but substituted**



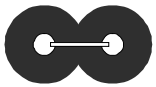
Policy Processing Business Requirements

- **Provide the answer to the question: What policies is the certificate chain good for? In other words, what policies or their equivalents are asserted in all the certificates in the chain**
- **Provide the answer in terms of relying party domain**
- **Permit (but do not require) policy processing to complete even if there is policy failure**
- **Has the infrastructure mandated that the chain be used in conjunction with an explicit policy? (Null policy does not always mean path failure)**
- **Issuer CA must assert issuer domain policy(s) only (business and potential legal reasons)**



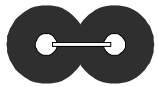
Policy Processing Inputs

- ***initial-policy-set:*** **The policies acceptable to application. Could be *any-policy***
- ***initial-explicit-policy-indicator:*** **A flag that determines if the path must be good for an explicit policy**
- ***initial-inhibit-policy-mapping-indicator:*** **A flag that determines if policy mapping is inhibited**



Policy Processing Outputs

- **Success or failure**
- ***require-explicit-policy:* A flag indicating if the infrastructure set the requirement for explicit policy**
- **A set of policies (in terms of the relying party domain) the chain is good for**
- **A subset of *initial-policy-set* the chain is good for**
- **Policy qualifiers and mapping history for the set of policies the chain is good for**



Policy Processing Algorithm Overview

- **Start with *any-policy and r*emove policies that do not appear in the next certificate**
- **Delete mapped policies in a certificate, if policy mapping inhibited**
- **Remove policies that are not in the *initial-policy-set* (after processing all the certificates)**
- **If explicit policy required and chain is good for no policies, policy error**
- **policyConstraints extension and related state variable processing remains same as the 12/97 Amendment**
- **Detailed algorithm available**